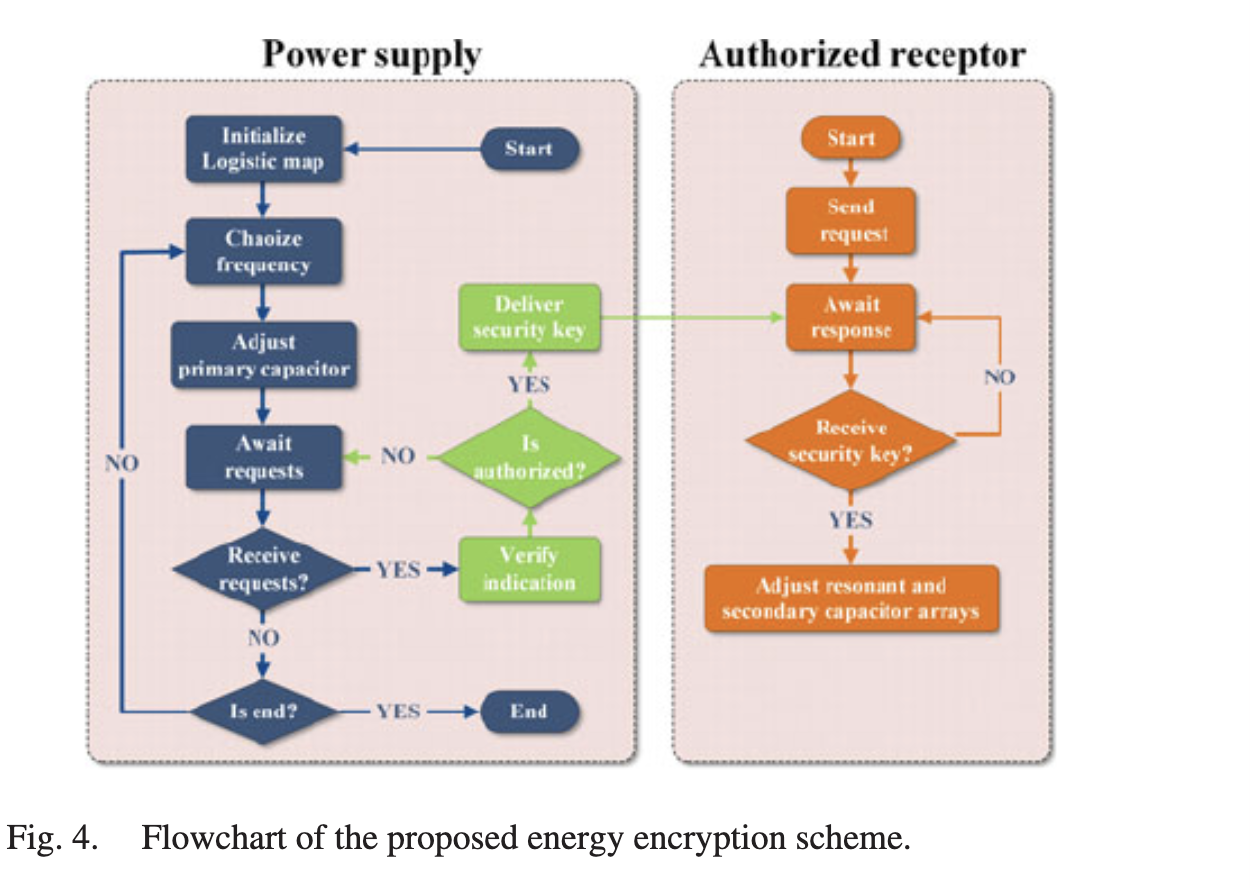
<https://www.embedded.com/infineon-adds-secure-authentication-to-wireless-charging/>

<https://tlo.mit.edu/technologies/cryptography-system-wireless-charging-modules>

According to these two articles, most efforts at adding encryption methods to wireless charging include multiple public keys on the receiver and a private key on the transmitter that allows both devices to verify that they are running the Qi 1.3 standard. This protects devices from malicious fake chargers and signal injection. This allows can stop small-scale battery damage and could potentially allow for power to be transferred over a longer range. However, the threat of snooping still exists. If an attacker intercepts the messages being sent and observes the individual packets, sensitive information could still be lost.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6928497>

This article proposes that the frequency of the energy transferred by the transmitter chaotically regulated. The power supply provides the security key, which is obtained by the authorized device. The authorized device can adjust the circuit to decrypt the energy. Unauthorized devices cannot obtain energy without knowledge of the security key, preventing unauthorized devices from stealing energy, intercepting packets, or injecting packets.



<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7976787>

This article proposes certificateless cryptography with two phases: 1) an authenticating phase that ensures certificateless authentication and key exchange between the power transmitter and the power receiver and 2) an encryption phase which makes use of the obtained session key in the first phase. It also explores how exactly the encryption allows for authentication of authorized devices before the session key is exchanged.

<https://duo.com/decipher/understanding-bluetooth-security>

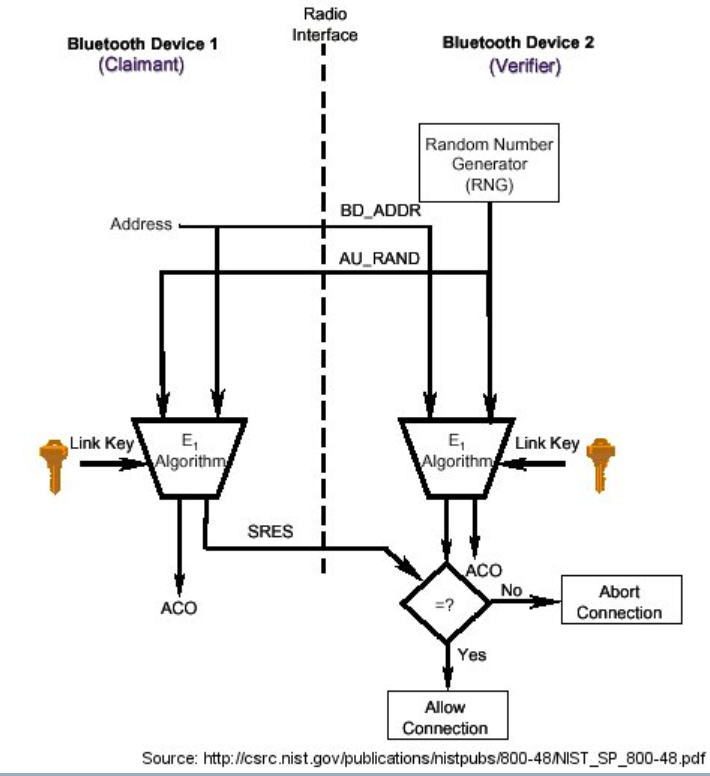
Looking into how Bluetooth implements security features such as encryption and authentication

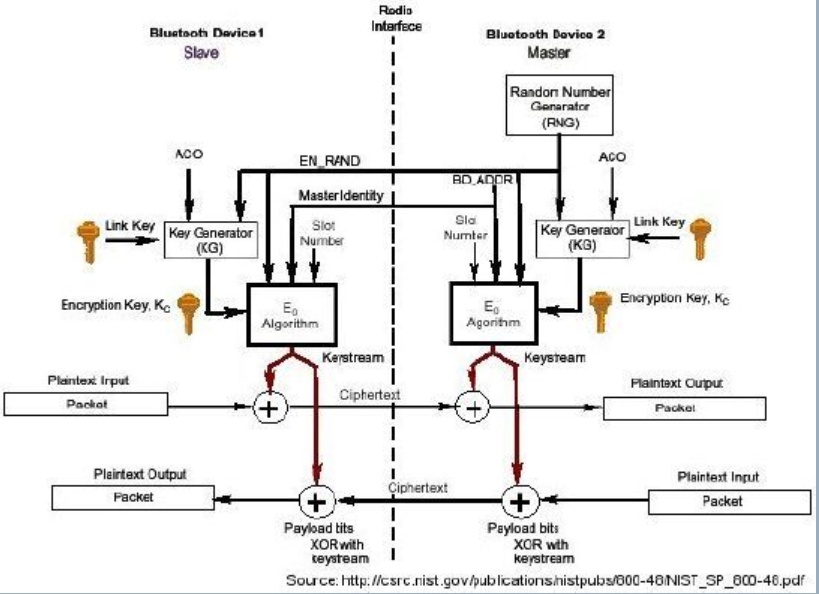
Want to look into possibility of Bluetooth tunneling to send qi data

<https://www.digikey.com/en/articles/inductive-versus-resonant-wireless-charging>

A possible modelling for using bluetooth in this way is by looking at resonant wireless charging vs the inductive system we have been using so far. This article displays the difference in hardware composition as well as how they handle device interaction. The article states that bluetooth is used as the communication standard for resonant devices.

Bluetooth as an example:





<https://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/wireless-computing/sec_bluetooth.shtml>